The Patent Office

PCT/GB 99/02671
12 AUGUST 1999

INVESTOR IN PEOPLE

4

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

GB99/2671

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

I also certify that the attached copy of the request for grant of a Patent (Form 1/77) bears a correction, effected by this office, following a request by the applicant and agreed to by the Comptroller-General.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Signed

Dated 16 AUG 1999

This Page Blank (uspto)

Patents Form 1/77

t 1977
e 16)

THE PATENT OFFICE
D
20 AUG 1998
RULE 57
RECEIVED BY POST

The Patent Office

20 AUG 1998

1/77

9
21AUG98 E384808-4 D02846
P01/7700 25.00 - 9818188.6

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

9818188.6

The Patent Office

Cardiff Road
Newport
Gwent NP9 1RH

1. Your reference

PLB/CC/N460

2. Patent application number
(The Patent Office will fill in this part)

NO 11/77 20/11/98.

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

~~UNDERSHAW GLOBAL LIMITED~~ COMODO TECHNOLOGY DEVELOPMENT LIMITED
TRIDENT CHAMBERS
PO BOX 146
WICKHAMS CAY
ROAD TOWN
TORTOLA
~~BRITISH VIRGIN ISLANDS~~

THE FOLD
3 CITY LANE
INALIFAX
~~HX1~~ HX3 5ZC

Patents ADP number *(if you know it)* 07594257001

If the applicant is a corporate body, give the country/state of its incorporation

~~BRITISH VIRGIN ISLANDS~~ UK

4. Title of the invention

COMMUNICATION SYSTEM, APPARATUS AND METHOD

5. Name of your agent *(if you have one)*

APPLEYARD LEES

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

15 CLARE ROAD
HALIFAX
WEST YORKSHIRE
HX1 2HY

Patents ADP number *(if you know it)* ~~AA005~~ 190001.

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

YES

Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	15 x 2
Claim(s)	
Abstract	
Drawing(s)	4 x 2

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	
Request for preliminary examination and search *(Patents Form 9/77)*	
Request for substantive examination *(Patents Form 10/77)*	
Any other documents *(please specify)*	

11. I/We request the grant of a patent on the basis of this application.

Signature Applegarth Legg Date 7 AUGUST 1998

12. Name and daytime telephone number of person to contact in the United Kingdom

PAUL BRANDON
0161 228 0903

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.

b) Write your answers in capital letters using black ink or you may type them.

c) If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.

d) If you have answered 'Yes' Patents Form 7/77 will need to be filed.

e) Once you have filled in the form you must remember to sign and date it.

f) For details of the fee and ways to pay please contact the Patent Office.

IMPROVEMENTS IN AND RELATING TO ELECTRONIC SECURITY DEVICES

Field of the Invention

The present invention relates to electronic security devices and to methods of operation of electronic devices.

Background to the Invention

Despite the growing proliferation of computer hardware and software, there are still serious problems associated with the security of both of them. Many new problems have arisen and others have become exacerbated as computers have become progressively more portable.

The present invention aims to provide in preferred embodiments thereof, electronic security devices that address at least some of the problems of the prior art.

Summary of the Invention

According to the present invention in a first aspect, there is provided an electronic security device comprising means for receiving and outputting signals when in an activated state, a real time clock for determining whether a predetermined real time period has expired and, if so, seeking an authorisation, means for verifying the authorisation, and means for deactivating the device in the event that a correct authorisation is not received in time.

This device provides time-limited security based on a real time measure, not based on the last use of the device.

Suitably, the device is adapted to receive encrypted authorisation codes.

Suitably, when not authorised the device received input signals, encrypts them and outputs the encrypted signals.

Suitably, the device includes means for generating a random (which expression includes pseudo-random) number and means for encrypting the random number. Suitably, the device includes means for performing a predetermined mathematical operation on the random number. Suitably, the device includes means for encrypting and decrypting data. Suitably, the encryption is according to a public key algorithm.

Suitably, the device additionally comprises a means for periodically checking the real time clock against a predetermined time period. Suitably, the periodic checking means comprises a counter which upon reaching a predetermined number initiates the check and means for re-setting the counter.

Suitably, the device comprises a dedicated power supply. Suitably, the device is embodied in a plug-in module, which plug in module suitably comprises a power source such as a battery.

According to the present invention in a second aspect, there is provided an electronic apparatus comprising a security device according to the first aspect of the invention.

Suitably, the security device is located between an electronic output device and an electronic input device.

The output device may, for instance, be a keyboard or a modem. The input device may be a central processing unit, memory unit, video card etc.

According to the present invention in a third aspect, there is provided a digital electronic computer comprising a security device according to the first aspect of the invention.

According to the present invention in a fourth aspect, there is provided a method of operating an electronic device comprising a security device which receives output signals when in an activated state, the method comprising the steps of using a real time clock to determine whether a predetermined real time period has expired and, if so, seeking an authorisation, checking whether the authorisation is acceptable and deactivating the device in the event that a correct authorisation is not received in time.

Suitably, the authorisation code is encrypted.

Suitably, when not authorised the device receives input signals, encrypts them and outputs the encrypted signals.

Suitably, the device generates a random (which expression includes pseudo-random) number and encrypts the random number. Suitably, the device performs a predetermined mathematical operation on the random number. Suitably, the device encrypts and decrypts data. Suitably, the encryption is according to a public key algorithm.

Suitably the encrypted number is transmitted to a verification station which verification station decrypts the encrypted number and verifies it against a number previously supplied to the electronic device.

According to the present invention in a fifth aspect, there is provided an electronic system operating according to the method of the fourth aspect of the invention.

Brief Description of the Figures

The present invention will now be described, by way of example only, with reference to the Figures that follow; in which:

Figure 1 is a schematic illustration of an electronic data processing apparatus embodying the present invention.

Figures 2A-2C are flow diagrams illustrating a mode of operation of the Figure 1 apparatus according to the present invention.

Description of the Preferred Embodiments

In one preferred embodiment of the present invention, there is provided an electronic data processing apparatus, typically a personal computer ("PC") 2. The PC 2 receives input signals from peripheral input devices (eg keyboard, data socket (modem), pen, voice recognition microphone etc). The PC includes a keyboard 4 having an associated keyboard controller 6 and a bus 8 forming an input channel.

A security device 10 is located between the keyboard controller 6 and the bus 8. The device is shown

schematically in the control line, but normally it will be located elsewhere, for instance in the body of the keyboard itself. The security device 10 has the following characteristics.

(i) It includes a real-time clock powered by an internal power-supply.

(ii) It includes a fast and reversible encryption/decryption algorithm such as DES or T-code (in ROM - read only memory).

(iii) It has a slower but more secure public key encryption/decryption algorithm having an associated public key (in ROM). Although referred to as a public key, it will not normally be disclosed.

(iv) It has a volatile memory Random Access Memory (RAM) including authorisation codes or an algorithm therefor, or pre-stored password and means for checking whether an input password or code matches such an authorisation code or password. The RAM is maintained by the power supply.

(v) It has the capacity to perform predetermined mathematical operations (in ROM and/or a 280 processor).

The security device 10 can be embodied in a board including a microprocessor (eg 280), read only memory, random access memory and a power source such as a battery to provide constant power for the real-time clock. If the

power source for the real-time clock is removed the security device 10 will become deactivated.

Generally, the security device 10 is activated by an activation code. The activation code is provided to the security device 10 encoded using a public key algorithm for high security. If the activation code is not provided on demand the security device 10 will enter an encryption state. The security device 10 is configured so that upon receipt of the correct activation code it is activated for a period of time determined according to the activation code, according to the in-built real-time clock. The period of time can be varied based upon the activation code received. While activated, the security device 12 transmits received signals unaltered. When not activated it is in the encryption state and encrypts signals passing therethrough. Thus, while in the encryption state the PC 2 cannot understand the output of keyboard 8.

When the predetermined period of operation expires, the security device 10 requests a further activation code for the next period. The code is requested by the user from a central database. The central database checks to determine if a further activation can be approved, for instance it may check to determine whether the device has been reported stolen, rental fees due have been paid etc. If further activation is authorised, the database encrypts the activation code for the next period using the particular security device's public key which is entered into the security device 10. The encrypted activation code normally is provided via electronic means directly to the security device 10, for instance directly by modem or over the internet, but can also be entered manually by the user, via a disk or by local infra red transmitter. Upon receipt of the encrypted activation code, the security

device 10 decrypts it and checks it against its pre-stored codes to determine the further predetermined period for which it is to be activated before requiring a further activation code.

Further security can be provided by an additional step of the security device 10 creating a random number which is encrypted according to the particular security devices public key. The encrypted random number is transmitted to the database centre (by whatever method). The database centre decrypts the random number, performs a predetermined mathematical calculation upon it (this could be as simple as to multiply by two or to XOR it with a key) and encrypts the new value with a public key provided (or its own public key) by the centre and sends it back to the security device 10. The security device upon receipt of the information, decrypts it using the relevant public key and compares the figures (after reversing the predetermined calculation or taking it into account). If the figures correspond then the security device 10 is confident it is dealing with the correct database centre and will accept reconfiguration instructions eg re-setting the real time clock.

If a correct activation code is not provided to the security device 10 on demand at the end of the predetermined period it becomes deactivated and will no longer correctly onward transmit received signals or transmit them at all. Normally, the security device 10 will demand an activation code some time prior to the end of the predetermined period of operation so that any errors or administrative difficulties can be resolved before the device becomes deactivated.

The PC may seek automatically an authorisation code, for instance via direct modem or internet access to an authorisation centre, without the user intervening.

Each PC normally will only have one such security device 10, but each such device manufactured has a different public key so each one is unique. Thus, generally each device will output a different signal upon receipt of the same input signal.

The device also provides password verification and can be configured to do this with or without the activation code.

In use, the PC 2 is configured to require a password before permitting access to certain functions or data. By way of example, a word-processing file may be password protected. Before permitting access to the file, the PC Central Processing Unit (CPU) requires confirmation from the security device 10 that the correct password has been entered.

Referring to Figures 2A-2C of the drawings that follow, there is shown a flow diagram of the operation of the present invention. The flow diagram shows a system configured to require correct password input for operation from power up and when a predetermined time period expires.

Referring now to Figure 2A, from power up 100 the security device 10 checks (101) a flag to determine whether it is its first power up in which case a configuration set-up is initiated (103). In CONFIGURATION the device is allocated its unique public key and the real-time clock is initialised. Other features such as

its predetermined mathematical operation, codes for certain time periods, etc can be configured or modified at this time. When configuration is finished or following the "password tamper count" is checked 102. At 104 if the tamper count is greater than the default tamper count a "LOCKED" message is displayed 106 and the security device 10 is configured into a "PASSWORD LOCKED WAITING" state (see Figure 2B) at 108.

If at 104 the tamper count is less than or equal to the default tamper count a password is requested 110. If at 112 the password is incorrect the tamper count is incremented by one 114. Otherwise, if the password is correct the security device 10 compares the current real time with the time against which activation has been permitted 116. If at 118 the time has expired, the security device is configured into the "LOCKED WAITING" state 120 (see Figure 2C) but if the time has not expired the information is passed without interruption (122).

Referring to Figure 2B, the "PASSWORD LOCKED WAITING" state is now described.

In the "PASSWORD LOCKED WAITING" state 108, at 124 the user is required to input a command instructing the PC to communicate with an authorisation centre. At this stage the user can choose manual or automatic communication with the authorisation centre. When the command is entered, the tamper count is incremented (126). If (128) the tamper count has expired the device is locked (130). If the tamper count has not expired, the device is allowed (132) to operate for a further 3-4 hours to enable the verification procedure to be completed.

The security device first creates and encrypts a random (or pseudo-random) number and encrypts it with the embedded public key (134). The encrypted random number is transmitted to the authorisation centre which may be automatic, for instance via a direct modem or the internet, or manually, for instance by the user phoning up the authorisation centre and entering what they are told via the keyboard. If the user communicates manually, further security can be implemented such as checking the users pre-allocated password etc.

The security device 10 then at 136 enters a waiting state to receive a data string (138) from the authorisation centre which its decrypts. If the received data is verified (140) the "wrong password tamper count" is incremented (142) and the device is permitted to operate for a further period with a new password that is notified to the user (144). The input from the authorisation centre includes an activation code and a new password encrypted according to the public key of the security device 10. If at 140 there is an error, indicating perhaps an attempted tampering with the device, it returns to the "PASSWORD LOCKED WAITING" state and asks for a command to be entered.

The authorisation centre will only provide the security device 10 with the necessary authorisation code and new password if approved. Approval may depend upon payment of relevant fees to the authorisation centre, checking whether the item of equipment is registered as stolen, or other security checks.

Referring to Figure 2C the security device 10 is in the "LOCKED WAITING" state 120. As this state is

indicative of a possible security breach, a higher level of security is adopted.

At 146 the security device 10 requires a command to be entered instructing it to communicate with the authorisation centre via modem (for instance). Upon receipt of the command 148, the tamper count is checked 150. If the tamper count is less than or equal to the DEFAULT valve the ALLOW TAMPER COUNT counter is incremented 152 and the device is authorised 154 to operate for 3-4 hours from then until the user downloads an acceptable activation code. Next, or if at 150 the ALLOW TAMPER COUNT is greater than the default value, at 156 the security device 10 creates a random (or pseudo-random) number which is encrypted using its public key. The encrypted random number is transmitted to the authorisation centre together with an identifier of the security device 10 in question.

The security device 10 then enters 158 a waiting state during which it expects to receive a data string from the authorisation centre for activation. The authorisation centre first checks whether the security device 10 can be authorised for a further period, for instance by checking whether it has been reported stolen or if any monies due are outstanding. If further use can be authorised, the authorisation centre (knowing the public key of the security device 10) decrypts the encrypted random number, performs a predetermined mathematical operation upon it (eg XOR or multiply), re-encrypts the result using the same public key and transmits the encrypted result with an encrypted new authorisation code to the security device 10 as a data string.

Upon receipt 160 of the encrypted data string, the random number is checked 162 (since the security device 10 knows the predetermined mathematical operation undertaken by the authorisation centre) and if verified the ALLOW TAMPER COUNT is incremented by one 164 and the device is authorised (166) for a further 3-4 hours until the user downloads a good activation code.

If the data is incorrect, a communication command is requested 146 once again.

Once in normal operation the device 10 uses a counter to count up to a predetermined value at which point the real-time clock is checked against its memory for authorisation of a further period. After each check the counter is re-set and counts again. Thus, the real-time clock is checked periodically against the permitted time of operation to determine if further authorisation is required.

Further embodiments of the present invention provide the security device 12 before a hard disk or other memory device in a PC architecture.

In this mode, the device encrypts signals input to the hard disk or other memory device and decrypts signals output from the same. This makes theft of data from the hard disk or other memory device harder, especially when the mode is combined with the feature described below. We refer to this as Auto-Encrypt On Demand Decrypt (AEODD).

The device can be placed before any essential integer of the PC, such as the hard disk, the CPU, the video card etc and configured so that it will only operate upon periodic receipt of an authorisation code. When correctly

activated the device onwards transmits received signals. If it is deactivated it blocks received signals. Alternatively, in the case of a memory device, encryption and decryption can be provided.

In each case, the provision of the device means that unless it is correctly activated the PC cannot properly be used. For instance, in the case of the hard disk option, everything that is written to the hard disk is encrypted (providing additional security to the data on the disk) using the fast encryption algorithm and everything read from it is decrypted by the device. The decryption only occurs if the device is activated so if the PC is stolen, then when the permitted time period expires no further authorisation can be obtained (with the assumption that the PC has been reported as stolen), so in effect it will become inoperative. Since activation relies on the public key encryption code, it is relatively secure. Equally, if the device precedes the CPU or video card, if it becomes deactivated, the PC is inoperative.

Deactivation of the security device can be by configuring it so that it no longer transmits signals upon deactivation, but the present invention is not limited to this alternative. Deactivation can also be achieved, for instance, by configuring the device to output a useless signal, for instance an encrypted version of the input signal.

Although reference is made herein to a "password", that can comprise any signal or combination of signals and need not be a "word" at all.

It will be appreciated by those skilled in the art that the device can be located in other positions or,

preferably, incorporated integrally within an essential element of the PC.

In a preferred embodiment of the present invention a microprocessor security device is provided with a real-time clock on a PC motherboard at a vital point, such as prior to the CPU, the video card, the hard disk etc. When correctly activated, the device receives and outputs received signals. The device remains activated for a predetermined period of time. Upon or just prior to expiry of the predetermined period, the device seeks an authorisation code that can be input to it in any of the known ways. If a correct authorisation code is not entered, the device is deactivated and no longer properly outputs received signals. Thus a periodic authorisation code is required to keep the security device, and hence the PC, operational.

In preferred embodiments, the authorisation code is provided in encrypted form and, if desired, a further authentication step can be carried out.

The invention is applicable to any electronic apparatus. Although the present invention is described in relation to a PC, it will be appreciated that in relation to the periodic activation code feature it can find application in any electronic apparatus, for instance a video camera, lap top computer, mobile telephone etc.

The reader's attention is directed to all papers and documents which are filed concurrently with or previous to this specification in connection with this application and which are open to public inspection with this specification, and the contents of all such papers and documents are incorporated herein by reference.

All of the features disclosed in this specification (including any accompanying claims, abstract and drawings), and/or all of the steps of any method or process so disclosed, may be combined in any combination, except combinations where at least some of such features and/or steps are mutually exclusive.

Each feature disclosed in this specification (including any accompanying claims, abstract and drawings), may be replaced by alternative features serving the same, equivalent or similar purpose, unless expressly stated otherwise. Thus, unless expressly stated otherwise, each feature disclosed is one example only of a generic series of equivalent or similar features.

The invention is not restricted to the details of the foregoing embodiment(s). The invention extends to any novel one, or any novel combination, of the features disclosed in this specification (including any accompanying claims, abstract and drawings), or to any novel one, or any novel combination, of the steps of any method or process so disclosed.

Fig 1

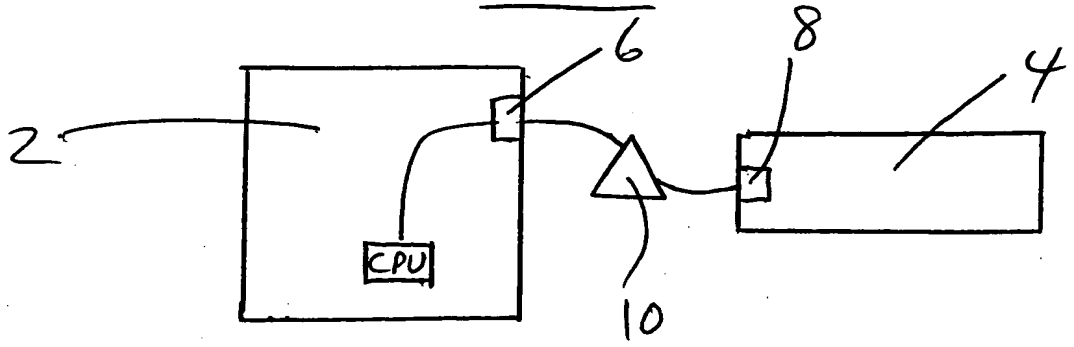


Fig 2A

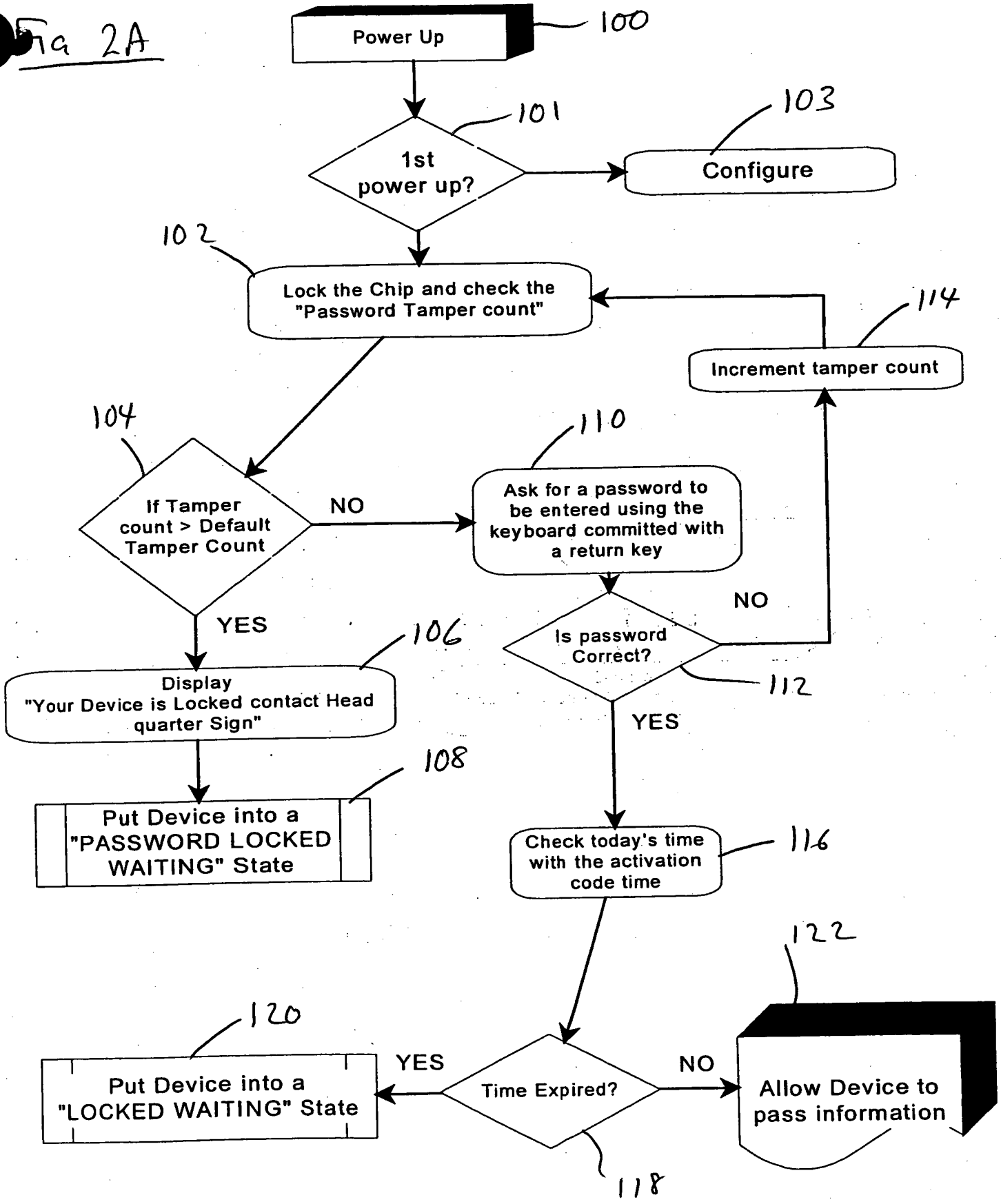

Power Up
100
1st power up?
101
Configure
103
Lock the Chip and check the "Password Tamper count"
102
Increment tamper count
114
If Tamper count > Default Tamper Count
104
NO
Ask for a password to be entered using the keyboard committed with a return key
110
YES
Is password Correct?
112
NO
YES
Display "Your Device is Locked contact Head quarter Sign"
106
Put Device into a "PASSWORD LOCKED WAITING" State
108
Check today's time with the activation code time
116
Time Expired?
118
YES
Put Device into a "LOCKED WAITING" State
120
NO
Allow Device to pass information
122

Fig 2B

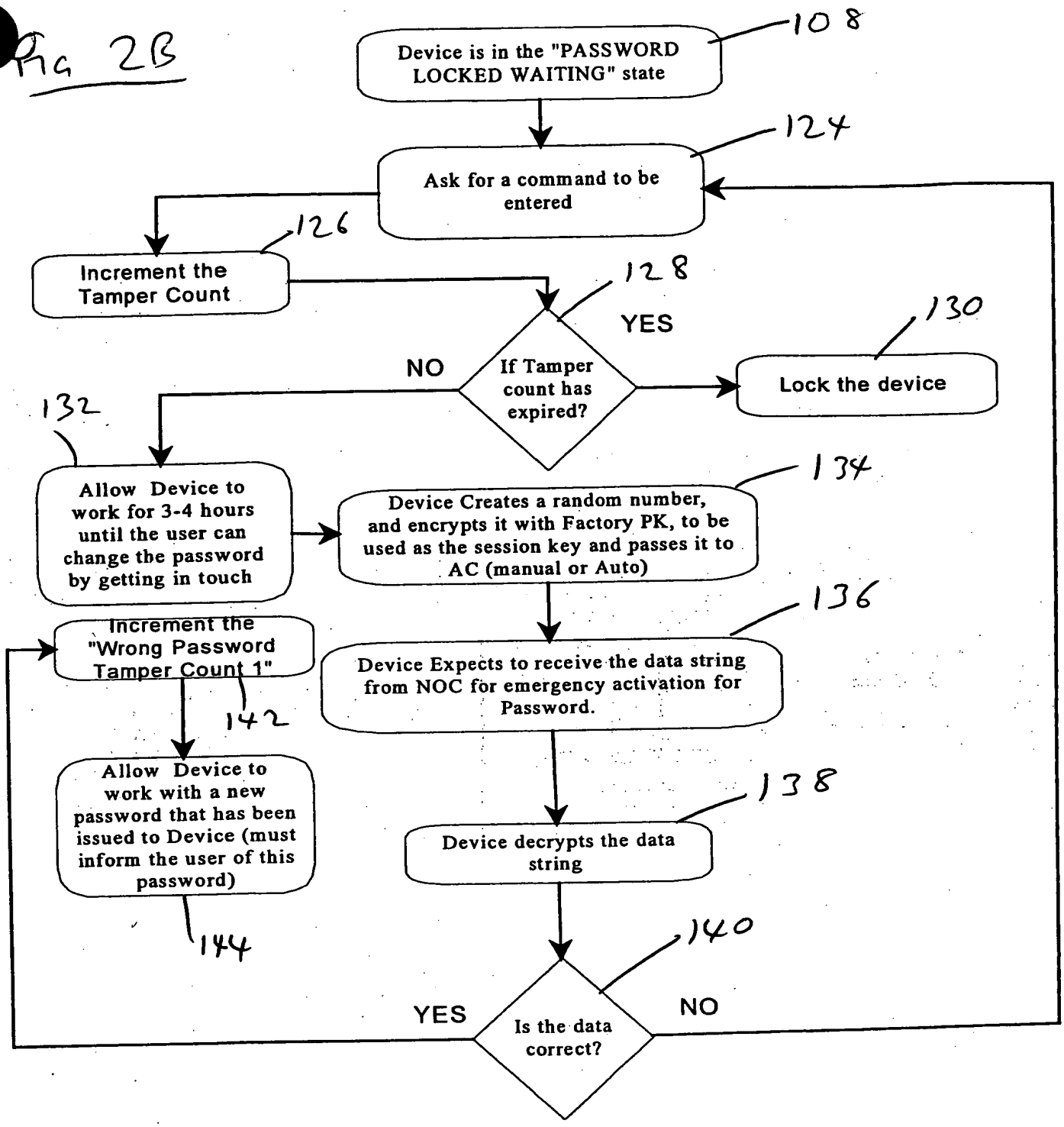
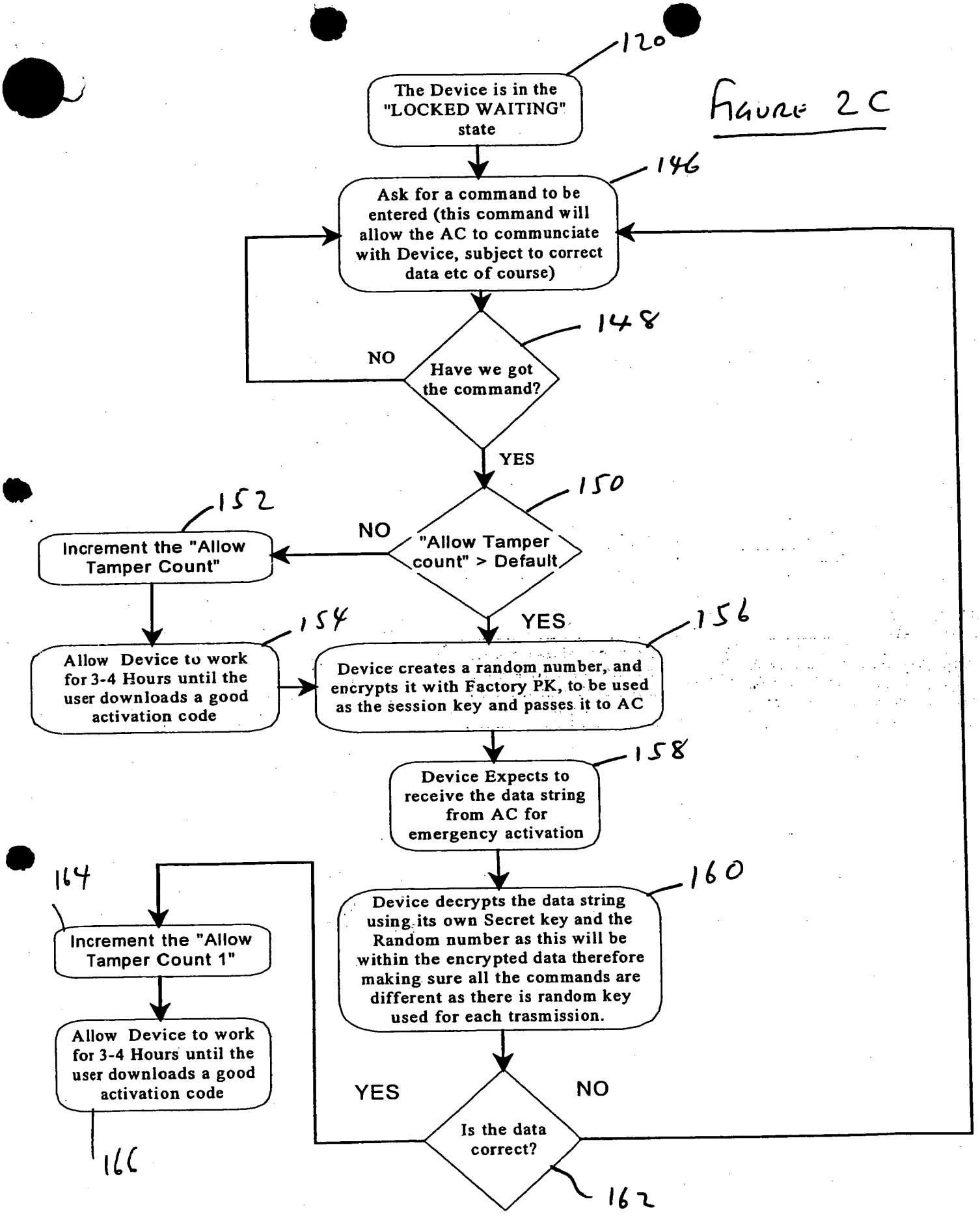

Device is in the "PASSWORD LOCKED WAITING" state
108
Ask for a command to be entered
124
Increment the Tamper Count
126
If Tamper count has expired?
128
YES
NO
Lock the device
130
Allow Device to work for 3-4 hours until the user can change the password by getting in touch
132
Device Creates a random number, and encrypts it with Factory PK, to be used as the session key and passes it to AC (manual or Auto)
134
Device Expects to receive the data string from NOC for emergency activation for Password.
136
Device decrypts the data string
138
Is the data correct?
140
YES
NO
Increment the "Wrong Password Tamper Count 1"
142
Allow Device to work with a new password that has been issued to Device (must inform the user of this password)
144

FIGURE 2C


120
The Device is in the "LOCKED WAITING" state
146
Ask for a command to be entered (this command will allow the AC to communciate with Device, subject to correct data etc of course)
148
Have we got the command?
NO
YES
150
"Allow Tamper count" > Default
NO
YES
152
Increment the "Allow Tamper Count"
154
Allow Device to work for 3-4 Hours until the user downloads a good activation code
156
Device creates a random number, and encrypts it with Factory PK, to be used as the session key and passes it to AC
158
Device Expects to receive the data string from AC for emergency activation
160
Device decrypts the data string using its own Secret key and the Random number as this will be within the encrypted data therefore making sure all the commands are different as there is random key used for each trasmission.
162
Is the data correct?
YES
NO
164
Increment the "Allow Tamper Count 1"
Allow Device to work for 3-4 Hours until the user downloads a good activation code
166